Israel Law Review **48**(1) 2015, pp 39–54. © Cambridge University Press and The Faculty of Law, The Hebrew University of Jerusalem, 2015.
doi:10.1017/S0021223714000272

The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives

Heather A Harrison Dinniss[*]

Cyber warfare and the advent of computer network operations have forced us to look again at the concept of the military objective. The definition set out in Article 52(2) of Additional Protocol I – that an object must by its nature, location, purpose or use, make an effective contribution to military action – is accepted as customary international law; its application in the cyber context, however, raises a number of issues which are examined in this article. First, the question of whether data may constitute a military objective is discussed. In particular, the issue of whether the requirement that the definition applies to 'objects' requires that the purported target must have tangible or material form. The article argues on the basis of both textual and contextual analysis that this is not required, but it contends that it may prove to be useful to differentiate between operational- and content-level data. The article then examines the qualifying contribution of military objectives such as their nature, location, purpose or use, and questions whether network location rather than geographical location may be used as a qualifying criterion in the cyber context. The final part of the article addresses the question of whether the particular ability of cyber operations to effect results at increasingly precise levels of specificity places an obligation on a party to an armed conflict to define military objectives at their smallest possible formulation – that is, a small piece of code or component rather than the computer or system itself. Such a requirement would have significant implications for the cyber context where much of the infrastructure is dual use, but the distinction between civilian objects and military objectives is a binary classification.

Keywords: cyber military objective, distinction, object, materiality, network location

1. Introduction

Cyber warfare and the advent of computer network operations have forced us to look again at the concept of the military objective. The definition provided in Article 52(2) of Additional Protocol I[1] to the Geneva Conventions defines military objectives in the following manner:

> In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

[*] Senior Lecturer in International Law, International Law Centre, Swedish National Defence College; heather.harrison-dinniss@fhs.se. An earlier draft of this article was presented as a paper at the 8th Annual Minerva/ICRC Conference, 'IHL: Military Objectives and Objects of War: An Uneasy Relationship', 24–25 November 2013, Minerva Center for Human Rights, The Hebrew University of Jerusalem, Israel.

[1] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I or AP I) (entered into force 7 December 1978) 1125 UNTS 3.

The definition reflects customary international law.[2] While some systems and networks – such as military communications networks, command and control systems and similar – comfortably fall within the established definition, cyber operations and the cyber environment in general raise unique challenges for the application of the definition in military operations. Cyber operations are those which use cyber capabilities with the primary purpose of achieving objectives in or through the use of cyberspace.[3] Usually this will take the form of a data stream used to affect the hardware and software resident in computers, computer systems, their component parts and wider networks. In particular, the advent of cyber operations raises the question of whether virtual targets, consisting primarily of data, can meet the definition of a military objective. The problem is compounded by the dual-use nature of much of the cyber infrastructure as well as the increasing virtualisation of data storage and networking. We live in a world which is increasingly characterised by virtual infrastructure – the idea of abstracting or separating software from hardware. Common examples of virtualisation include using services in the cloud, using virtual private networks (VPN) or similar to extend a local area network beyond its physical location, or by making use of virtual machines to efficiently run and separate functions within a given physical system. This trend is occurring not only for end-user services like email or various forms of social media,[4] but also for parts of states' critical infrastructures as well as military apparatus and systems. The move towards virtualisation means that more of the data, processes and code that parties to an armed conflict may wish to target with cyber operations are no longer tied to a single, dedicated and identifiable piece of hardware; for example, a single server or other platform may run multiple 'instances' of an operating system (or indeed different operating systems), each dedicated to a separate function. In the event that only one of these instances needs to be neutralised in order to achieve the aim of the intended operation, the correct identification of the appropriate military objective for a cyber operation is determinative of the permissible damage to civilian objects in the proportionality calculation.

The author has previously discussed the topic of legitimate military objectives for cyber warfare.[5] The present article returns to some of those discussions and addresses some additional issues raised in light of the approach taken by the authors of the Tallinn Manual[6] with the intention of fleshing out the debate on these topics. The article is divided into three interlinking parts in order to address key issues that are raised by cyber operations in respect of the legitimate

[2] Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law, Vol 1: Rules* (International Committee of the Red Cross and Cambridge University Press 2005, revised 2009) (ICRC Study) r 8.

[3] Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press 2013) (Tallinn Manual) 258.

[4] Social media may be divided into six main categories: collaborative projects (eg Wikipedia), blogs and microblogs (eg Twitter), content communities (eg YouTube), social networking sites (eg Facebook), virtual game worlds (eg World of Warcraft) and virtual social worlds (eg Second Life): Andreas Kaplan and Michael Haenlien, 'Users of the World, Unite! The Challenges and Opportunities of Social Media' (2010) 53 *Business Horizons* 61, although the boundaries between these categories are becoming increasingly blurred.

[5] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 184.

[6] Tallinn Manual (n 3).

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

targets of military operations as defined by Article 52(2) of Additional Protocol I. Before discussing the issues raised in relation to military objectives of cyber operations, the article first examines the concept of data and suggests that a useful distinction may be made between different types of data: the content and operational levels. The article then addresses the issue of the materiality of military objectives. In particular, it is argued that, contrary to the suggestion of the ICRC Commentary[7] and the Tallinn Manual, the reference in the definition to the term 'object' does not impose a requirement that a military objective must have a tangible form. It illustrates that the laws of armed conflict have successfully dealt with intangibility both historically and in the modern context. The article then examines the four criteria by which objects may qualify as military objectives and, in particular, examines the idea of network location as a means of possible qualification. Finally, the article turns to the scope of the military objective and the level of specificity at which it must be defined. The author argues that the principles of proportionality and precaution may also be viewed as imposing limits on the definition of the objective and suggests this approach as a means of constraining the problem of extensive dual-use infrastructure.

2. A QUESTION OF DATA

Most discussions regarding military objectives and cyber operations come up against the question of whether data per se can constitute a military objective.[8] Indeed, this question underlies the argument of most of this article; at the outset, however, it is important to clarify terminology. Whereas most discussions of this nature tend to treat data as a single entity, the author finds it useful to make a distinction throughout between different types of data: content-level and operational-level data. Content-level data – such as the text of this article, or the contents of medical databases, library catalogues and the like – is largely excluded from the ambit of this article. That is not to suggest that content-level data may never be protected under international humanitarian law, but the data sets that would be the subject of the most concern are already covered by the specific protections granted, for example, to medical records and material, and cultural property (for demographic data and archives).

Operational-level data – also known as logical-level data or, more commonly, program data – is essentially the 'soul of the machine'. It is this type of data that gives hardware its functionality and ability to perform the tasks we require. Operating systems, software applications and SCADA systems[9] are all examples of operational level-data. To avoid confusion, throughout this article operational-level data will simply be referred to as 'code'.

[7] Yves Sandoz, Christophe Swinarski and Bruno Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (International Committee of the Red Cross and Martinus Nijhoff 1987) (ICRC Commentary).

[8] See, eg, Noam Lubell, 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?' (2013) 89 *International Law Studies* 252, 267; Tallinn Manual (n 3) 127.

[9] SCADA (Supervisory Control and Data Acquisition) systems provide real-time data analysis of complex systems, reporting back to a central hub where they may be monitored and controlled.

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

From a conceptual point of view, making a distinction between these two types of data is important because of the different types of harm that are likely to result from damage, destruction or neutralisation of each type. As a general rule, destruction of operational-level data or code will result in loss of functionality of the system, whereas similar destruction of content-level data will leave the system intact, albeit with corrupted or missing data.[10] Although there is very little state practice in the area, the way in which states have tended to conduct and react to low-level cyber operations to date tends to suggest that loss of content-level data is viewed differently from operations which involve loss of functionality of the system. While the majority of the authors of the Tallinn Manual were of the opinion that data should not be considered an object (see the discussion at Section 3 below on materiality), a minority of the experts involved in drafting the Tallinn Manual considered that, for the purposes of targeting, data per se should be regarded as an object.[11] Their grounds for objecting to the exclusion of data from the notion of an 'object' was that failure to do so would mean that loss or deletion of extremely valuable and important civilian datasets could escape the reach of the law of armed conflict.[12] While these concerns are not without merit, given the difference in how states have thus far treated attacks on content-level data as distinct from code, the present author considers that including *all* data within this scope may be too broad. Such an expansive inclusion would take the definition of a military objective too far from its purpose in identifying the legitimate targets of attacks and military operations. The comments of the minority are indicative of the difficulties created by failing to distinguish between two different types of data and adopting an overly broad definition of data such as that adopted by the Tallinn Manual. The glossary of the Manual refers to data as 'the basic elements that can be processed or produced by a computer'; it thus incorporates both content-level and operational-level data. The author considers that the conflation of these types of data creates unnecessary difficulties in interpretation which may be usefully resolved by regarding each type separately.[13]

3. Materiality of Objectives: The Requirement of 'Objectness'

One of the problematic aspects of the Tallinn Manual is an apparent inconsistency in the approach adopted by the group in dealing with some of the underlying concepts of cyber warfare. In this instance it is the treatment of intangibility in the object requirement of the definition of military objectives. The opening clause of Article 52, 'in so far as *objects* are concerned' (emphasis added), caused the majority of the international group of experts to consider that the term 'object' required the particular item to be something 'visible or tangible', as suggested

[10] As a side note, content-level data is also the most common type of data to be backed up by organisations and individuals.
[11] Tallinn Manual (n 3) 127.
[12] ibid.
[13] As noted, this article will not consider the protection of certain types of content-level data other than to reiterate that some types will already be covered by protection of items such as medical records and cultural archives.

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

by the text of the ICRC Commentary to the Additional Protocols.[14] Thus, for the purposes of the Manual, only the hardware components of cyber infrastructure (such as servers, routers and sensors), computers and computer systems may constitute objects and therefore military objectives. Interestingly, the Manual makes no distinction between virtual and physical cyber infrastructure in the black-letter rule, merely listing it as something that may be included in the definition of a military objective. It is only in the Commentary to the rule that the discussion surrounding the object requirement of the definition makes clear that the majority of the Tallinn group considered that it must include 'visible and tangible' physical components rather than merely lines of code.

It is notable that the references provided by the ICRC Commentary when discussing the meaning of the term 'object' (or, in the French text, '*biens*') are merely to the dictionary definitions of the term rather than to any specific discussions that occurred in either the working committees or the Diplomatic Conference regarding the matter.[15] It is indisputable that the dictionary definitions of both the English and French terms, as referred to in the ICRC Commentary, refer to material things that are perceivable by the senses. The present author considers it clear from the text of the Commentary that the definitional point about the term 'object' was being made merely to distinguish the term as a 'thing' from its use in the sense of 'aim or purpose' (for example, of a military operation) rather than to specifically exclude intangible objects from the definition.[16] Thus any computer program, database, system or virtual network could still qualify as a legitimate target if it meets the two-part definition set out in Article 52(2), regardless of whether it has a tangible component or exists purely as lines of code.[17] The author stands by this interpretation; however, the fact that the majority of the group behind the Tallinn Manual reached a different conclusion makes it worth revisiting the criterion in more depth. The first point of note is that while it may lack materiality, code is certainly perceivable by the senses and by sight, in particular, and may hence be considered visible. It is thus the relevance of the materiality or tangibility of the object that is in question with regard to the definition of military objective.

The rules contained in the Tallinn Manual are intended to reflect customary international law. However, given the fact that the accepted customary international law definition of a military objective is based on the treaty definition set out in Article 52(2) of Additional Protocol I, one must look at how that term is defined to determine what was intended to be included.

The English version of the ICRC Commentary is derived from the French original, published in 1986. As a historical side note, it is worth remembering that this is the year in which TCP/IP protocols were standardised (allowing considerably more networks to connect with one another), two years before the first internet-based attack, and three years before the invention of the world wide web.[18] It is self-evident that the 1977 Additional Protocols and their ICRC Commentary

[14] ICRC Commentary (n 7) paras 2007–08; Tallinn Manual (n 3) 126
[15] ICRC Commentary (n 7) paras 2007–08.
[16] Harrison Dinniss (n 5) 184; for a similar analysis see Lubell (n 8) 267.
[17] Harrison Dinniss (n 5) 184.
[18] The TCP/IP protocol (a suite of protocols or rules sets for communicating data across platforms) was standardised in 1986, allowing different networks to link with each other in a standardised way and develop eventually to form the international system of networks that we know now as the internet. The final barriers to

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

could not possibly have contemplated the incredible changes the internet revolution would have on society (and the corresponding development of the law regulating it) and the sheer number of things that would operate on the basis of underlying computer code, nor would they have envisaged the current trend towards virtualisation which separates software and hardware even further.[19]

Treaty terms must be interpreted in good faith and in accordance with their ordinary meaning in their context and in the light of their object and purpose.[20] While, at the time of drafting in 1977, it is likely that this limited objects to material items in an attempt to exclude such 'objectives' as civilian morale and, in the wake of the Second World War, aerial bombing campaigns, code is by no means such an amorphous concept. As noted above, code is patently visible, although it may lack tangibility in the sense of being able to be touched or having a physical presence outside the electromagnetic spectrum.[21] Throughout the whole body of laws of armed conflict there is an underlying dichotomy not only between civilian and military in terms of distinction but also between the treatment of people and the treatment of things. It is this second underlying dichotomy that this debate taps into – regardless of its intangibility, code is nevertheless a thing. It does not equate with the somewhat notional targets of civilian morale, a population's willingness to fight, or the even less specific 'victory' – all of which formed the historical backdrop to the attempts to define military objectives which culminated in the definition adopted in the Additional Protocol.

Further, and perhaps most importantly, requiring tangibility in today's world leads to a manifestly unreasonable result. To take a practical example, weapons, weapons systems and military *matériel* are perhaps the epitome of a legitimate military objective. Malware that is designed specifically to cause death, injury, destruction or damage is indisputably a weapon.[22] Examples include Stuxnet-type code, which is intended to cause physical destruction,[23] or even viruses such as Wiper, which destroyed the functionality of computer systems without destroying any

commercialisation of the internet were removed in 1995, leading to the exponential growth of networked technologies, and the ability for cyber warfare to even exist. The first internet-based attack occurred in 1988 – the Morris worm – which caused disruption to major portions of the then internet.

[19] It is to be hoped that the current project under way by the ICRC to update the commentaries will contain scope for these changes.

[20] Vienna Convention on the Law of Treaties (entered into force 27 January 1980) 1155 UNTS 331, art 31. The International Court of Justice has recognised in multiple cases this principle of treaty interpretation as reflective of customary international law and has extended its application as a general rule of interpretation beyond treaties to include Security Council resolutions such as the statutes of the International Criminal Tribunals for the former Yugoslavia and Rwanda.

[21] Note that this has not prevented courts from holding electronic data to be a tangible thing for the purposes of certain domestic legislation; see, for example, cases concerning s 215 of the United States Patriot Act holding electronic records to be 'tangible things' for the purposes of that Act.

[22] For a discussion on weapons intangibility see Harrison Dinniss (n 5) 68; Tallinn Manual (n 3) 141–42.

[23] Stuxnet is the name given to the malware that is responsible for physical damage being caused to nearly 1,000 enrichment centrifuges at the Nantanz Uranium enrichment facility in Iran. Discovered in 2010, it is widely believed to be the work of the United States and Israel working in cooperation. Neither state has commented publicly on the matter. For technical details on the attack see Nicolas Falliere, Liam O'Murchu and Eric Chien, 'W32. Stuxnet Dossier: Version 1.4', February 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

physical components.[24] However, by excluding intangible objects such as code from the interpretation of the definition offered by the majority of the Tallinn group, neither of these cyber weapons would constitute a legitimate military objective. It cannot be correct that one can have a weapon that is made entirely from code that does not constitute a military objective.

As the definition of civilian objects is provided in a negative form – that is, civilian objects are all things that are not military objectives[25] – we are left with two main alternatives. Either a piece of code such as Stuxnet is a civilian object or, given that the problem is with the term 'object' itself, it is not covered by the definition of military objectives at all. Given that the object and purpose of both the principle of distinction and of the Additional Protocol itself[26] is to provide effective protection for civilians and civilian objects while enabling parties to an armed conflict to conduct effective military operations, either of those alternatives produces a manifestly unreasonable result. In order to conduct efficient military operations against cyber targets while minimising the harm to civilians and civilian objects, it will sometimes be necessary to conduct attacks against code rather than the physical infrastructure on which it rests. Any modern interpretation of the law should reflect this necessity and allow for that to happen.

An alternative reading rests on the wording of the opening sentence of Article 52(2): attacks shall be strictly limited to military objectives. While the second sentence of the definition of military objectives is limited to objects by the phrase '[i]n so far as objects are concerned', the first sentence contains no such limitation.[27] Yoram Dinstein argues that it is through this distinction that the definition can be viewed as including enemy combatants.[28] It is tempting to make a similar argument for those intangible items such as code, for which it is argued that they do not fulfil the materiality requirement of the definition. In that manner the general rule contained in the first sentence is not constrained by the more specific definition contained in the second. While Dinstein's argument is compelling when considering *people* as military objectives and therefore legitimate objects of attack, applying this reasoning to intangible objects in order to avoid the definitional problem under discussion is problematic. It does not sit easily with the underlying

[24] Wiper is a mysterious and sophisticated piece of malware, discovered in April 2012, which rendered computer systems unbootable by wiping sections of the hard drives. The main computer systems affected by the virus were businesses and government departments associated with oil production in Iran. Unfortunately, as very little data survived the attacks, little is known about the malware itself but experts have cited possible links to the Duqu software, largely believed to be the work of the United States and Israel. See, generally, Kaspersky Lab, Global Research and Analysis Team, 'What Was That Wiper Thing?', *SecureList*, 29 August 2012, https://www.securelist.com/en/blog/208193808/What_was_that_Wiper_thing. Wiper appears also to have inspired copycat attack, Shamoon – an attack launched against Saudi Arabia's leading oil company, Saudi Aramco, as well as RasGas in Qatar.

[25] AP I (n 1) art 52(1).

[26] ICRC Commentary (n 7) para 3685, stating that the object and purpose of AP I is to 'improve the protection provided by the [Geneva] Conventions to the victims of international armed conflicts'. For a detailed treatment of the Vienna Convention on the Law of Treaties as an interpretive tool for determining cyber military objectives see Kubo Mačák, 'Military Objectives 2.0' (2015) 4(1) *Israel Law Review* 55.

[27] The Tallinn Manual makes no distinction between the two sentences in its restatement of this rule as it relates to cyber.

[28] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (2nd edn, Cambridge University Press 2010) 92.

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

dichotomy within the law between people and things. In addition, the fact that the tangibility requirement merely comes from an interpretation contained in the text of the 1986 Commentary than from a specific discussion in the Diplomatic Conference merely adds to the present author's conclusion that in relation to cyber operations the term 'objects' must be interpreted to include intangible things such as code.

INCONSISTENCY

It seems likely that the position of the majority of the Tallinn Manual group on the materiality requirement for objectives is linked to the requirement for physical effect in the definition of attacks.[29] After all, the primary purpose of the definition of a military objective is to enable the principle of distinction to be applied in attacks (or other military operations).[30] However, by insisting on tangibility at the definitional stage, they have complicated the matter unnecessarily and created an inconsistent approach to materiality both within the text of the Manual and within the broader approach to the law of armed conflict. Two different examples of the approach to intangibility are illustrative.

Neither the text of the Tallinn Manual nor the laws of armed conflict more generally take issue with the concept of intangibility when it comes to weapons. States have no difficulty in determining that chemical and biological weapons fall within the purview of the law despite the fact that a number of them are largely intangible in nature,[31] a fact which is noted by the Tallinn Manual group.[32] Similarly, the fact that some forms of laser technology (which, like code, utilise the electromagnetic spectrum) are considered as weapons indicates that the intangibility of the process is not in issue. The Tallinn Manual itself defines cyber means of warfare as including any 'device, material, instrument, equipment, *or software* used, designed or intended to be used to conduct a cyber attack'.[33]

The issue of intangibility has also been considered by courts and tribunals dealing with items that are subject to protection under the laws of armed conflict in respect of property offences. The Nuremburg war crimes tribunals in both the *Krupp* and *IG Farben* trials following the Second World War found the defendants guilty of property offences despite the intangible nature of

[29] Tallinn Manual (n 3) r 30.

[30] For a discussion of the difference between attacks and operations see Harrison Dinniss (n 5) 196–202 and Heather A Harrison Dinniss, 'Attacks and Operations: The Debate over Computer Network "Attacks"', paper presented at the conference 'New Technologies, Old Law: Applying International Humanitarian Law in a New Technological Age', 28–29 November 2011, Minerva Center for Human Rights, The Hebrew University of Jerusalem, http://www.academia.edu/4086617/Attacks_and_Operations__The_debate_over_computer_network_attacks.

[31] For example, dispersible poison gases may be detectible only at the molecular or atomic level. The question of whether a determination of tangibility or intangibility should be made at the atomic or sub-atomic level is beyond the scope of this article. However, the fact that such gases are contained in a physical canister prior to dispersal is no different conceptually from code being contained in the physical infrastructure of a computer system.

[32] Tallinn Manual (n 3) 106.

[33] ibid 142 (emphasis added).

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

the property in question,[34] holding that the intangible nature of the property (in those cases, shares and other corporate property rights) was no barrier to individual criminal responsibility under modern international law. As with weapons, members of the Tallinn Manual group were prepared to conclude that digital property – in particular, digital cultural property – although intangible, was protected under the laws of armed conflict.[35]

Despite the different circumstances of both weapons and property, it seems clear that both states and courts do not have a problem with intangibility per se, where the law allows for such an interpretation and the object and purpose of the law are served by doing so. Similarly, the Tallinn Manual group also accepted that both the means of inflicting harm (cyber weapons) and some of the intended targets of that harm are not limited by their intangibility. It therefore appears inconsistent to insist on tangibility in the permitted targets of cyber operations when the law is capable of such an interpretation. The context and purpose of providing a definition of military objectives was to increase the *effective* protection for civilian objects through better compliance with the principle of distinction. In a world increasingly characterised by dual-use technology and an intensifying trend towards virtualisation of infrastructure (including critical infrastructure), an interpretation that would prevent states from refining the definition of a military objective to its narrowest possible form (discussed in Section 5 below) is counter-productive.

4. QUALIFICATION OF OBJECTIVES: NATURE, LOCATION, PURPOSE OR USE

The definition also requires that, in order to qualify as a military objective, an object must, by its nature, location, purpose or use, make an effective contribution to military action.

Those objects which by their *nature* make an effective contribution to military action include all objects which have an intrinsically military character. With respect to cyber operations, this category would include all weapons, weapons systems and *matériel*, sensor arrays, battlefield devices, military networks and databases, military command and control systems, communications systems and any other digital device purposely built to military specifications.[36] It would also include those objects directly used by the armed forces: weapons, equipment, transport, fortifications, depots, buildings occupied by armed forces, staff headquarters and communications centres.[37]

A civilian object will become a military objective through use when it is *used* for military purposes. Classic examples include military use of civilian transport, airfields or the use of

[34] *Trial of Alfied Felix Alwyn Krupp Von Bohlen Und Halbach and Eleven Others* (*The Krupp Trial*), Law Reports of Trials of War Criminals, United States Military Tribunal, Nuremburg Vol X, 164; *Trial of Carl Krauch and Twenty-Two Others* (*IG Farben Trial*), Law Reports of Trials of War Criminals, United States Military Tribunal, Nuremburg Vol X, 46.
[35] Tallinn Manual (n 3) r 82.
[36] With the exception of medical devices, networks, etc.
[37] ICRC Commentary (n 7) paras 2007–08.

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

buildings to house military personnel or supplies. The cyber infrastructure that serves those objects will similarly become a military objective when used for military purposes. In an age of dual-use infrastructure, in which large amounts of military traffic and communications are sent across civilian networks, this becomes particularly problematic and exposes vast amounts of that infrastructure to attack. Social media sites, such as Facebook and Twitter, may also become open to attack where they are used to organise and coordinate military operations.[38] However, given the specificity requirement outlined above – to refine the target so as to minimise harm to civilians – only those sectors of the structures that are actually used should be targeted. Such objects regain their civilian status once they are no longer used for military purposes.

An object will qualify as a military objective through the *purpose* criterion where the intended future use of the object is military. Intention is notoriously difficult to assess, however, and parties must take care in determining the actual intentions of the opposing forces rather than the potential use of a particular object (for example, a piece of cyber infrastructure) and establishing that a civilian object is intended for military use.

The criterion of *location* was introduced without explanation into the definition of military objective in Article 52(2) by Working Group III. However, during the Diplomatic Conference several states made comments to the effect that the amendment recognised their position that a specific area of land might qualify as a military objective (independently of its nature or use) where, because of its location, its total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage.[39] The ICRC Commentary to the Article goes on to explain that a site might have special importance for military operations because it is a site that must be seized or because it is important to prevent the enemy from seizing it, or otherwise because it is a matter of forcing the enemy to retreat from it.[40] Such land areas generally qualify because of a specific geographical feature, such as a mountain pass. Physical cyber examples are not easy to come by given the distributed nature of networks, which are specifically designed with efficiency and redundancy in mind.[41] However, in terms of geographical location, a civilian WIFI network located in an area in which an enemy is operating may enable the enemy to piggy-back communications on the signal, for example. Denying the enemy use of the network may give a direct and concrete advantage to the attacking forces.[42]

[38] The posting of steganographically altered images on social media sites is a fairly well known tactic among organised armed groups.

[39] See, eg, explanations of the vote by the United Kingdom (169), Canada (179), Federal Republic of Germany (188), the Netherlands (195) and the United States (204): CDDH/SR41, *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Geneva (1974–1977)* (Federal Political Department 1978) Vol VI.

[40] ICRC Commentary (n 7) paras 2020–24.

[41] That is, if one path to a destination is inaccessible data can be sent via an alternative route. Indeed, different packets of information (eg pieces of a message or data request) may be sent via different routes and reassembled at the destination address.

[42] Although note that from an operational perspective, there may be more value in intercepting and monitoring communications.

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

A more interesting question is whether an object may qualify as a military objective through its *network* location rather than its location in physical space.[43] As noted, the classic example of a military objective is the mountain pass or defile; another would be a trail through swamp or jungle.[44] Cyber infrastructural equivalents of such geographical features may include internet kill switches, undersea cable landing points or primary nodes of a state's internal telecommunications networks, each of which would make an effective contribution to military action. Similarly, the recent revelations regarding NSA and GCHQ data collection have brought into public awareness the strategic importance of certain internet switches which have allowed the intelligence agencies to access all data travelling across them. Denying particular data routes to military traffic by neutralising particular network nodes, thus forcing the traffic over less secure or monitored switches, would provide a definite military advantage. Subject always to the principle of proportionality, there is no reason why a particular node's network location should not form the basis for attacks on such targets by analogy, although in practice it is likely that such strategic objects would qualify also through purpose or use.

Finally, while accepting the customary status of the definition of military objective in Article 52(2), the United States has adopted a broader definition of the effective contribution to military action requirement to include those items which make an 'effective contribution to the enemy's war fighting or war sustaining capability'.[45] Thus, according to this interpretation 'economic objects of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability may also be attacked'.[46] Such an approach moves the lawful targets of attack away from the close nexus with military action that is required by the definition contained in Article 52(2). Taken to its logical extreme, under such an interpretation not only the political command and control structures become targetable, but a vast array of civilian activity, including those that merely contribute to the economy through taxes, could be construed as indirectly supporting or sustaining the war effort. It is notable that the majority of the Tallinn Manual group also came to this conclusion, finding that the connection between war-sustaining activities and military action was too remote.[47]

Regardless of how an object makes its effective contribution to military action – whether it qualifies through its nature, location, purpose or use – it must also meet the second arm of the definition to be considered a legitimate military objective. The total or partial destruction, capture or neutralisation of the object must offer a definite military advantage in the circumstances ruling at the time. It is widely accepted that the military advantage may be determined from the attack as a whole and not from isolated parts;[48] thus a particular cyber operation may form part of a broader operation and be measured accordingly.

[43] Harrison Dinniss (n 5) 185.
[44] Dinstein (n 28) 128.
[45] US Navy, US Marine Corps and US Coast Guard, *The Commander's Handbook on the Law of Naval Operations*, NWP 1-14M/MCWP 5-121/COMDTPUB P58007A, 2007, para 8.2.
[46] ibid para 8.2.5.
[47] Tallinn Manual (n 3) 131.
[48] See statements made by Australia, Belgium, Canada, France, Germany, Italy, the Netherlands, Nigeria, Spain and the United Kingdom in the state practice accompanying ICRC Study (n 2) r 8.

5. SPECIFICITY OF OBJECTIVES: CODE, COMPONENT, SYSTEM, NETWORK

The above discussion on materiality is linked with a second aspect brought to the fore by the specific ability of cyber operations to target increasingly smaller parts of a system in order to achieve the desired military outcome. The precision of such specific operations raises questions about the appropriate scope of the definition within the cyber context and the precise level at which the military objective should be defined – code, component, system or network level. Clearly each situation will be highly dependent on the type of objective to be attacked and the desired outcome of the operation. This section will explore some of the different ways in which an objective might be defined and examine whether the principle of proportionality and the requirement to take precautions in attack can offer insights into the appropriate level of specificity required in defining the military objective.

Although not a problem exclusive to cyber operations, the level of specificity of the definition is of particular relevance in cyber operations because of the high level of interdependence between civilian and military cyber infrastructure. The majority of modern militaries, particularly in an age of defence budget cuts, do not construct their own completely separate cyber infrastructure. Instead they rely primarily on the cables, routers, switches and satellites (as well as the firmware and software that run them) that are used for civilian communications.[49] While the term 'dual use' is a useful descriptor of those systems and infrastructure that have both civilian and military uses, it is not a term that appears in the law of armed conflict. The negative definition of civilian objects (that is, all objects that are not military objectives) ensures that the classification of objects is binary – either something is a military objective or it is a civilian object. Once something qualifies as a military objective – either through its nature, location, purpose or use, and its destruction, damage or neutralisation provides a military advantage – it remains targetable for the entire time that it meets that definition. Further, it becomes a legitimate target of attack in its entirety (except where separable parts remain civilian – for instance, different buildings of a hospital).[50] Any remaining effect on civilian functions that the object may retain must be taken into account during the proportionality assessment and the requirement to take precautions in attack, rather than qualification under the principle of distinction. However, the amount of civilian function that is to be assessed depends on the level at which the object is defined. Consider, for example, a particular dual-use system or network which includes a switch that contains

[49] For example, in 2010, the former US Director of National Intelligence, Admiral Michael McConnell, estimated that 98 per cent of US government communications, including classified communications, travel over civilian-owned-and-operated networks and systems: Michael McConnell, Former Director of National Intelligence, Keynote Address at the Texas Law Review Symposium 'Law at the Intersection of National Security, Privacy, and Technology', 2 February 2010, cited in Eric Jensen, 'Cyber Warfare and Precautions against the Effects of Attacks' (2010) 88 *Texas Law Review* 1533. Civilians also make use of some military infrastructure: eg the GPS satellite network is used for a huge range of civilian applications.

[50] Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 *International Review of the Red Cross* 533, 562, and references therein.

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

altered code designed to copy and possibly amend data passing over the network for military purposes. If the military objective is defined at the system or network level, any civilian traffic or data that exists purely within the system or network becomes irrelevant to the calculation (as it forms part of the military objective and is therefore no longer civilian). If, however, the military objective is defined at the component (switch) or code (malware) level, the civilian traffic or data within the rest of the system or network remains outside the definition of the military objective and thus remains a civilian object which must be taken into account. Thus a question remains as to whether there is an obligation to *define* a military objective in its most minimal form? If so, in 'defining down', how far must one drill?

A traditional reading would suggest not. However, the requirements to take all feasible precautions in selecting both the means and method of attack[51] and also the choice of target where more than one is available for a similar military advantage will constrain states from launching attacks against targets that will cause excessive harm to civilians.[52] While these are features of the proportionality principle, in this case they appear to be inextricably linked to the definition of the military objective and the appropriate scope or specificity of the target selected. Where it is *possible* to identify the military objective as a distinct piece of code (for example, a virtual machine running inside a broader system), which will give a similar military advantage, Article 57(3) of Additional Protocol I requires the attacker to choose the objective that will result in the least danger to civilian lives and to civilian objects. Thus, in an age of dual-use infrastructure, the obligation on states to select targets that will cause the least harm to civilians will require states to reduce the harm to the civilian population through the operation of the obligation to take all feasible precautions in attack and select the target that will cause the least damage to civilians or civilian objects – that is, by defining the target at the minimum level possible: code, rather than network.

Is there thus a similar obligation when conducting reconnaissance on adversary computer systems to carve out and identify the particular aspects or sections of a system that will deliver the military advantage? There is a legitimate concern that the realities of military operations will not lend themselves to fine-tuning the military objective to such a specific level. However, the obligation arises only in the circumstances 'when a choice is possible',[53] thus providing a measure of discretion to attacking forces based on the underlying system and the purpose of the operation. Further, any state that is conducting cyber attacks must be capable of conducting sufficient network reconnaissance to meet its other obligations under the laws of armed conflict; it should therefore have the means or capacity to determine the most efficient method of inflicting the necessary damage while minimising civilian harm. It is far better to send a piece of malware similar to the Wiper algorithm against a cyber weapon such as Stuxnet[54] or a listening post such as

[51] AP I (n 1) art 57(2)(a)(ii).
[52] AP I (n 1) art 57(3) provides: 'When a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects'.
[53] ibid.
[54] The Wiper algorithm caused disruption to Iran's oil industry systems by wiping significant sections of the hard drives; for more details see Kapersky Lab (n 24).

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

Duqu or Flame (or weapon, had either of their latent attack-code components been activated) than to cause physical damage to the hardware.[55] This is particularly true where the targeted code is sitting on virtual infrastructure that can be migrated to an alternative in an instant or where the hardware or infrastructure that is affected is something that the state intends to utilise in the future.

Thus, in the same way that states with the ability to use smart munitions with a smaller payload have a corresponding obligation to select their military objectives with more specificity, and in such a way that 'target area' bombing is now almost entirely prohibited on the ground of being indiscriminate,[56] so too will states that possess the ability to define military objectives at a more specific level be required to do so through the operation of the principle of proportionality and the requirement to take all feasible measures in precaution in order to avoid, and in any event to minimise, harm to civilians. Thus the definition of military objectives must be sufficiently broad to cover both. It should be remembered, however, that systems, nodes,[57] components and code must still all qualify as military objectives (or not) on their own merits. It must also be recalled that the military advantage to be gained may also be part of a wider attack – for example, against a communication centre node which requires the neutralisation of multiple objectives to achieve the desired outcome.

Some guidance on the required specificity may also be found in Article 51(5)(a) of Additional Protocol I, which prohibits treating separate and distinct military objectives as a single objective as a form of indiscriminate attack – that is, the prohibition against target-area bombing.[58] This rule is recognised as a norm of customary international law in both international and non-international armed conflicts,[59] and also applies in the cyber context. The Tallinn Manual group was prepared to find that this rule would be breached when individual military (physical) components could have been attacked separately,[60] a conclusion with which the present author agrees, albeit one that should be extended to code and virtual infrastructure as well. As noted in the previous section, the fact that the relevant separate and distinct portion of the system consists of code should not relieve the state of its obligations.

[55] Duqu and Flame are both instances of malware designed primarily for espionage purposes. However, both pieces of malware contained latent components or modules that would allow them to be turned into sabotaging malware had that component been activated. In an example of the efficiency of sending code to attack such malware, many instances of Flame were removed, presumably by its creators, by sending a kill command which removed all traces of the malware from the computer.

[56] AP I (n 1) art 51(5)(a) provides, as an example of a prohibited indiscriminate attack, an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration or civilians or civilian objects. Dinstein notes that two exceptions remain: the first is where the military objectives in the area are not 'clearly separated and distinct' and, secondly, where there is no 'similar concentration of civilians or civilian objects': Dinstein (n 28) 119.

[57] A node is a connection or processing point in a given system or network; the exact definition will change depending on the type of network or system involved. Nodes may be virtual or physical.

[58] See n 56 above.

[59] ICRC Study (n 2) r 13 and associated practice.

[60] Tallinn Manual (n 3) 158.

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

There will be instances where particular code, whether it consists of virtual infrastructure or a particular piece of software, forming part of the military *matériel* of the adversary is discovered as part of an otherwise civilian object. A subsequent cyber operation to destroy the code would also cause destruction of some functionality of the remaining civilian host system (and thus meet the requirements of an attack). Yet it seems disingenuous to suggest that the attack is directed against the host system (even though it would qualify as a military objective through its dual use), where it is, in fact, more properly viewed as collateral damage in the attack against the military object embedded within. The Tallinn Manual approach to such a problem merely moves the alleged object of the attack to the nearest physical component or the recipient of the physical effect.[61]

Similarly there will be other instances where a physical component or the wider system is the appropriate minimum-level military objective; these will depend entirely on the system that is the target of the attack. For an attack like Stuxnet, specifying a particular component of the system to be attacked makes sense. In that case, the attack targeted switches that control the rotors which determine the spin rate of the uranium enrichment centrifuges in order to cause physical damage. However, once one starts attacking virtual infrastructure, it becomes more problematic: components may be a physical part of a device, or a small piece of code.[62] In other cases the wider system will be the appropriate target[63] – for example, the Blue Force tracking system or particular command and control systems.[64]

There is no doubt that in some cases an entire network will become a legitimate military objective: command and control networks of the armed forces, communication networks and defence department networks are all classic examples of networks that meet the definition and could all be attacked in their entirety. However, with the high percentage of military communications and traffic that also travel over civilian networks,[65] there is a very real threat that those networks will also be targeted as (legitimate) military objectives based on their dual use. The large amount of redundancy built into network design, particularly those interconnected networks such as the internet, makes it impossible to know with any certainly which routes any military data packets will take. Similarly, from a practical perspective, it is nearly impossible to determine in real time which are military packets and which are civilian; thus the entire network may become a military objective. As the Tallinn Manual notes, an analogy may be drawn with a road network. It is suggested that while this analogy is apt (or, indeed, comparisons with rail networks), state practice in relation to Article 57(3) on the choice of targets has shown belligerents choosing to attack a smaller part of the network in order to achieve the same military advantage.[66]

[61] ibid 108, referring to the object of attack.
[62] This article will limit itself to the physical type of component as the other is dealt with as code.
[63] The Tallinn Manual defines a computer system as consisting of one or more interconnected computers with associated software and peripheral devices. It can include sensors and/or (programmable logic) controllers, connected over a computer network: Tallinn Manual (n 3) 258.
[64] Blue Force tracking systems allow commanders to identify and locate friendly (and enemy) forces on the battlefield via GPS location and mapping software.
[65] See n 49.
[66] ICRC Commentary (n 7) paras 2226–28.

https://doi.org/10.1017/S0021223714000272 Published online by Cambridge University Press

For example, instead of neutralising the rail network by targeting railway stations, small but crucial switches away from civilian population centres were selected; a similar approach should be adopted with regard to communication or computer networks. Where the military use of the network can be isolated by attacking a particular internet switch, the military advantage will be achieved by considering the switch as the appropriate objective.

6. CONCLUSIONS

This article explores the legal issues surrounding the definition of 'military objectives' as they relate to cyber operations. It begins by suggesting that one should be careful not to define data too broadly as there is value in delineating between content-level data and logical or operational-level data or code. The article concentrates on whether or not code may qualify as a military objective.

The mere fact of intangibility should not per se preclude a piece of code from being a military objective if it meets the other criteria set out in Article 52(2) of Additional Protocol I. By using the term 'objects', the drafters sought to exclude notional targets such as civilian morale, and the interpretation provided in the Commentary seeks to distinguish objects as 'things' from the sense of 'aim or purpose'. Further, in today's world of increasing virtualisation and extensive interdependence between military and civilian infrastructure, requiring tangibility results in a manifestly unreasonable result. Such a result is inconsistent with other treatments of intangibility in international humanitarian law and contrary to the expressed purpose of providing effective protection to civilians and civilian objects.

Thus, regardless of its intangibility, code may qualify as a military objective by providing an effective contribution to military action either through its nature, location, purpose or use. Of particular interest in the cyber context is whether an object may qualify through location based on network location rather than physical space. This article accepts that the criterion is aimed at geographical features, but suggests that the same reasoning might also be applied to networks.

Finally, while there is no specific requirement in the principle of distinction to define a military objective at the minimum level possible, the principles of proportionality and the requirement to take all feasible precautions in attack to avoid and at least minimise harm to civilians and civilian objects operate to effectively constrain the definition. Where it is possible to define more than one military objective within a system and attack each separately, states are required to do so. It is suggested that explicitly recognising this obligation as part of the principle of distinction, particularly with regard to cyber operations, is one way of mitigating the effects on extensive dual-use cyber infrastructure in the modern era.